Department of Information Technology

# Y2K Times

2000

Volume 1, Issue 3 | *It's About Time!* | October 22, 1999

| *Until 2000...* | Days left: 71 | Working days left: 47 | Weekends left: 10 |
|---|---|---|---|

## *Message from the State CIO*

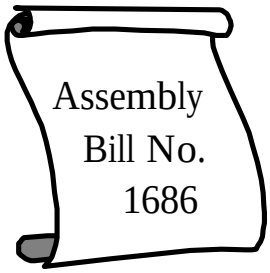
Now that all of the participating state entities have submitted their Continuity Plans for Business (CPBs), our next focus should be the protocols that entities will employ for communications during the rollover event. How and when will incidents, if any, be reported and escalated, and to whom?

While the DOIT is coordinating communications internal to the State, the Governor's Office of Emergency Services (OES) is coordinating all external communications surrounding the rollover event. If you have any questions for the OES, contact them at (916) 262-1843 or visit their web site at www.oes.ca.gov.

I encourage you to look at the DOIT's October 1999 Quarterly Report to view the status of all your hard work for the State. The most current data could not be collected by the reporting due date, so a Supplemental Report will be submitted to the Legislature on October 29th. This report will present CPB milestone results and the status of department critical remediation efforts.

**In This Edition of *Y2K Times* …**






## *Governor Davis Signs Bill to Continue the Department of Information Technology*

*In a move to keep the Department of Information Technology intact for another two years, Governor Davis recently signed into law Assembly Bill No. 1686. Below is the letter he wrote in this regard.*

October 8, 1999

To the Members of the Assembly:

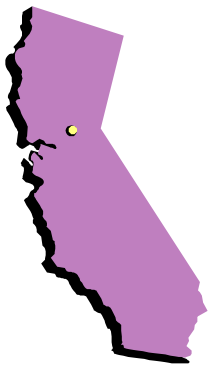
I am signing Assembly Bill No. 1686, which postpones by two years the sunset date which would eliminate the Department of Information Technology.

I believe that the Department of Information Technology has proven itself to be an indispensable leader of the State's technology management strategy. The department has shown extraordinary leadership and effectiveness in its stewardship of the state's Year 2000 Program. However, creating a sunset date for a department is highly unusual and potentially deleterious. It suggests a lack of commitment to the department's mission, which has affected employee morale and impacted the department's ability to attract and retain staff in a highly competitive environment.

Therefore, I intend to sponsor legislation in the next session that would eliminate the sunset date from the Department of Information Technology, thereby reassuring the present and future employees of the state's commitment to this department's vital mission on behalf of the people of California.

Sincerely,

GRAY DAVIS



## *California's Status at 97.1%*

California's mission critical systems are 97.1% remediated. The remaining 2.9% is expected to be complete before the year's end.



*"The information provided herein is a Year 2000 Readiness Disclosure pursuant to the Year 2000 Information and Readiness Disclosure Act (P.L. 105-271)."*

## Y2K Events: Past and Future

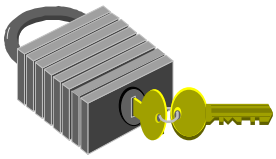
- On October 14, 1999, State CIO Elias Cortez and DOIT PIO Oscar Gonzales participated in the first of a series of four Y2K Legislative Staff Briefings designed to prepare the State Legislators' District Offices for inquiries from constituents regarding Y2K. Dates of the other briefings are as follows:

  October 19 – Cerritos Community College
  October 22 – CSU, Fresno
  October 29 – College of Marin

- On October 15, 1999 the DOIT submitted its October 1999 Quarterly Report to the Legislature.
- On October 18, 1999, the DOIT launched a redesigned Y2K web site. The web site is now structured to reach: State Legislators, State and local government, and the California public.
- On October 18, 1999, the Sacramento Bee newspaper published an article that conveyed how confident State officials are about California's systems:

  http://www.sacbee.com/voices/news/old/voices01_19991018.html

- On November 5, 1999 the CIO from California and its neighboring states will convene for a Roundtable session at which they will discuss regional Y2K issues.
- On November 21, 1999 the television network NBC will air "Y2K: The Movie" in which a computer scientist must "follow the sun" in an effort to avert a disaster.



## Y2K Insecurity?

The code is all fixed, the Operating System has been Y2K-patched, and the Business Continuity and Contingency Plans are all in place and tested. You have met all reporting requirements and have passed all Y2K assessments. You are ready for the rollover – but are you really? What is the status of your Information Security Program? Will poor security cause a problem during the rollover period? If so, will it be identified as a security problem or will it be viewed as just another Y2K problem?

Within the IT community there are varying opinions about the security risks associated with Y2K. Some analysts feel this will be a golden opportunity for hackers to cause significant disruption of IT services, theft of proprietary and/or confidential information, or financial fraud. Whether or not the risks are truly much greater during Y2K, these risks should not be taken lightly, and actions should be taken to prepare for and respond to actual or potential security breaches.

*Continued on page 3*

## Y2K Challenge Spans Several Years

The Y2K challenge does not end on January 1, 2000. The Gartner Group estimates that, worldwide, Y2K failures will be spread out over a number of years (see figure below). They estimate that only 10% of all Y2K failures will occur in the first two weeks of January 2000. If a full 30% of all failures occurred in 1999 and before, as they estimate, then if the volume of failures actually reported is any indication of the magnitude of the problem, it does not seem that another 25% more than that (to 55%), in 2000, will be much of a concern for the population in general.

It should be noted that most all **mission critical** systems will have been remediated by January 1st. Therefore, most failures that may occur throughout 2000 and beyond will only be **department critical** or **non-critical** (see "Y2K Definitions" on page 4).

| Year | Percent of all Y2K failures |
|---|---|
| Pre-1999 | 5% |
| 1999 | 25% |
| 2000 | 55%<br>(10% in the first two weeks of January) |
| 2001 | 15% |



*"The information provided herein is a Year 2000 Readiness Disclosure pursuant to the Year 2000 Information and Readiness Disclosure Act (P.L. 105-271)."*

## Y2K Insecurity? Continued from page 2

***What are the risks?***

In reality the security risks associated with Y2K are basically the same issues that we face daily in securing and protecting our technology, but there are a couple of new twists.

First of all, we have to ask ourselves: Is there a threat of a security system failing? If these systems provide access to applications, networks, services or facilities, can we log-in to the system or get into the building if the security system fails? Are there contingency plans in the event of their failure? Have these contingency plans been tested and proven to be effective in meeting the business needs? Are there any other issues that need to be addressed?

Second: Is there potential for problems associated with remediated applications or systems? Many outsourced remediation activities have provided the opportunity for outsiders (and insiders) to insert 'back-doors' or to place otherwise malicious code (virus and Trojan programs) to be executed during or after the Y2K roll-over event.

Finally, there is concern that the hacking community will generate an increased amount of malicious code and scanning/probing activity in search of vulnerable systems.

***What can we do?***

- Review your security standards and procedures. If there is a question about a system and its security – test it or have it assessed by a security professional.
- Activate appropriate systems and other logging facilities and proactively monitor these logs for signs of actual or attempted intrusions. If intrusions occur, seek qualified assistance and notify the local authorities.
- Ensure that all anti-virus, and other, software, such as intrusion detection systems, are up-to-date with the proper patches and signature files or databases. Keep these tools turned on and actively monitoring for malicious activity.
- Educate your user community about the importance of proper security practices. The real key to an effective Information Security program is the people working within business. With a heightened awareness, most security breaches or vulnerabilities can be caught and addressed before things get out-of-hand.
- Establish a security incident response team to take ownership of security incidents and responsibility for resolution. ¦

## The Prudent Planner

*The Prudent Planner presents State activities and events that you may see or hear about in the foreseeable future.*

- Now that almost all State entities have completed the interface testing among themselves, California's 58 counties have the next big effort. Our county governments would appreciate any help you can provide them, whether it's technical expertise/resources, volunteerism, or simply words of encouragement. Interfaces supporting law enforcement and the categorical aids are of particular importance.
- Y2K Information Technology Directive 1999-02 does not restrict State entities from purchasing new equipment or software. It cautions them about installing new purchases into already-Y2K-tested production environments.
- Some departments have already monitored hackers attempting to break into their systems. DOIT and the Trade and Commerce Agency have been surveying the virus detection industry for special precautions. If you haven't already, this is a good time to make awareness and education of this security issue a highlight of your Y2K program. (See "Y2K Insecurity?" beginning on page 2). ¦



*"The information provided herein is a Year 2000 Readiness Disclosure pursuant to the Year 2000 Information and Readiness Disclosure Act (P.L. 105-271)."*

## Y2K Definitions

**Mission Critical: Systems and Services** – A mission critical system or service is defined as an automated system or government function whose unavailability or failure, partial or complete, would significantly impact or impair the successful delivery of a vital government service or mission, as listed below:

| | |
|---|---|
| *Public Safety* | *Public Health* |
| *Law & Justice* | *Environmental Protection* |
| *Human Services* | *Mission Critical Operations* |

**Department Critical: Systems and Services –** A department critical system or service is defined as a business system or service whose failure would significantly impact and/or impair the successful mission of a specific State entity and its ability to operate in an effective, efficient, and cost effective manner to provide continuous, accurate and reliable services to its clients. Also, these systems and services do not meet the definition of "Mission Critical" above.

**Non-Critical: Systems and Services –** All systems and services that are not considered to be either Mission Critical or Department Critical.

## Y2K's Effect on Specific State Services

Specific questions should be directed to your department's Y2K project manager or to the State's Y2K Program Management Office at: Project.Office@emc.ca.gov. The Y2K PMO will be glad to answer any questions you may have and may address your concerns in subsequent newsletters.

## Interesting Reading

*The following are paths to interesting web sites.*

- General Service Administration – This site offers a collection of federal government links, including international, consumer, and community information, and Y2K for Kids:
  http://www.itpolicy.gsa.gov/mks/yr2000/y201toc1.htm
- Industry Search (NorthernLight) – Type "y2k" or "millennium bug" or "century date change" in the Search For box, and select an industry or "All Industries" to find articles on how business is managing Y2K:
  http://www.northernlight.com/industry.html
- Government Hotlines – This page links to U.S. Government telephone hotlines for consumer and small business information on Y2K:
  http://www.nist.gov/y2k/consumer.htm

## Web Sites for More Government Y2K Information

| | |
|---|---|
| California Year 2000 web site | http://www.year2000.ca.gov |
| Governor's Office of Emergency Services | http://www.oes.ca.gov |
| Federal Y2K web site | http://www.y2k.gov |
| County information | http://www.csac.counties.org/counties_close_up/county_web/index.html |
| City information | http://www.cacities.org/cities_online/cities_online.asp |
| United States Information Agency | http://www.usia.gov |

## Comments and Questions:

If you have any comments or questions regarding this newsletter, or any of its contents, please contact Lance Williams by one of the means below. If you would like to receive the newsletter by email, please send an email message, with your name, department, title, and email address to: Lance.Williams@doit.ca.gov, or call (916) 445-7020.

The newsletter and previous issues are available for download off of the DOIT's Year 2000 Publications web site, under the section titled "Y2K Times Newsletter":
*http://www.year2000.ca.gov/publications/*

*Please reduce, reuse, recycle*



*"The information provided herein is a Year 2000 Readiness Disclosure pursuant to the Year 2000 Information and Readiness Disclosure Act (P.L. 105-271)."*